**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**TITLE:**

# METHOD AND SYSTEM FOR A SET OF NETWORK APPLIANCES WHICH CAN BE CONNECTED TO PROVIDE ENHANCED COLLABORATION, SCALABILITY, AND RELIABILITY

**(PRIORITY OF U.S. PROVISIONAL NO. 60/264,445, FILED JANUARY 26, 2001)**

**INVENTORS:**

**Michael R. Primm**
**10237 Matoca Way**
**Austin, TX 78726**

**John J. Fowler**
**11914 Lincolnshire Ave**
**Austin, TX 78758**

**Gary Faulkner**
**12609 Chittim Circle**
**Austin, TX 78732**

**ASSIGNEE:**

**NetBotz Inc.**
**11044 Research Blvd.**
**Suite C-100**
**Austin, TX 78759**

CERTIFICATE OF EXPRESS MAILING UNDER 37 C.F.R. §1.10

I hereby certify that this correspondence, which includes 34 pages of specification, 6 pages of claims, 1 page of abstract and 9 sheets of figures and is being deposited with the United States Postal Service Express Mail Service under 37 C.F.R. §1.10 addressed to: Box Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231, on January 25, 2002.

Express Mailing Number: EV 011 384 880 US

Laura H. Andre

# METHOD AND SYSTEM FOR A SET OF NETWORK APPLIANCES WHICH CAN BE CONNECTED TO PROVIDE ENHANCED COLLABORATION, SCALABILITY, AND RELIABILITY

## TECHNICAL FIELD OF THE INVENTION

**[0001]** This invention relates in general to a method and apparatus for remote monitoring of a set of sensors. More specifically, this invention relates to a method and apparatus for communication between a cluster of network enabled devices and a remote monitoring facility.

## RELATED APPLICATIONS

**[0002]** This application claims priority of U.S. patent Application, Serial No. 60/264,445, filed January 26, 2001 entitled: "METHOD AND SYSTEM FOR A SET OF NETWORK APPLIANCES WHICH CAN BE CONNECTED TO PROVIDE ENHANCED COLLABORATION, SCALABILITY, AND RELIABILITY", and is incorporated herein by reference in its entirety.

## BACKGROUND OF THE INVENTION:

**[0003]** Data traffic on networks, particularly on the Internet, has increased dramatically over the past several years, and this trend will continue with the rapid growth of e-commerce and other services on the Internet requiring greater bandwidth. With this increase in data traffic on networks, there has been a corresponding increase in the number of computer equipment rooms, known as "server rooms," used to house the equipment necessary to support data traffic routing. Furthermore, the increasing dependency of companies on their Internet presence has created an urgency to keep the server rooms up and running at all times. Industry estimates show that there are over 400,000 such rooms currently in existence in the United States.

**[0004]** The growth in Internet traffic has prompted many businesses to construct a server room to allow their employees to access Internet information or enable e-commerce and store data. Once viewed as a goal, continuous server up time has become a necessity. Keeping track of numerous computers, along with associated bridges, routers, backup power supplies, etc., can be a formidable task. A large company with server rooms in more than one city might well be faced with spending thousands of dollars on software packages to keep their equipment running. Prices of $1,000 per computer are common. Dedicated technicians are also needed to monitor network equipment and issue work orders to repair failed units.

**[0005]** While reliable, modern computer systems cannot tolerate excess heat, dust or humidity. Heat can rapidly cause equipment deterioration. Failure of cooling fans can reduce equipment lifetime to days or hours. A single high-speed LAN (local area network) failure can cause slow system response. These and other such failures within the equipment in a server room occur routinely and can cause great disruption to a business.

**[0006]** Solutions do currently exist for monitoring computer networks and equipment to prevent such failures. However, these solutions are primarily targeted at high-end, very large systems such as those used by large corporations or institutions that have large budgets to support equipment monitoring. For example, Hewlett-Packard provides a high-end monitoring package with a starting price of around $250,000. In the middle tier, smaller monitoring solutions can be had for approximately $20,000. Some of these systems only permit inspection of devices on a local basis. Others permit a technician to inspect geographically diverse installations from a central console. However, all of these solutions are expensive to implement and complex and difficult to maintain and train personnel to use them.

**[0007]** As a result, small to medium companies having small to medium networks are left in the position of requiring a means to monitor and maintain their computer network equipment from failing while not having the resources to afford the high-priced solutions currently available. Many firms cannot afford a high-end solution or simply do not have the time and resources to train their IT personnel to learn and use complex systems. Instead, the common monitoring method in many such companies is user complaints to the IT manager to indicate when a problem has occurred. The idea is that someone in the organization will notice a failure and call for repairs before damage can be done. The reality, however, is that most IT managers have suffered some from of server room damage from excess heat or other physical phenomenon or simply just failure.

**[0008]** This is especially true for companies having multiple server rooms and that have concerns about routine access to each of these rooms. For example, most IT managers would like some form of remote access for determining the status of a server room. Additionally, concerns exist with current solutions regarding the manpower intensiveness of these solutions. Most network monitoring solutions can consume a full or part-time employee. The financial justification for these systems is, therefore, difficult because network equipment typically fails

yearly or on a disaster basis, and the cost of recovery is seen as less than that of maintaining a full-time employee to routinely monitor the equipment.

**[0009]** Similar concerns exist for monitoring rack-mounted components such that individual components within a rack can be monitored remotely. Also, current monitoring solutions do not provide for video imaging of remote server locations over a network. Computer equipment is typically placed in server rooms for two reasons: security and environmental control. Remote video imaging of a server room over a network can provide for maintaining security of the equipment despite the lack of a physical presence on site.

**[0010]** A typical computer room can house hundreds of devices, ranging from expensive server grade computers to bridges, routers, uninterruptible power supplies and telephone equipment. A server room's environment requires monitoring because out of limit environmental variables can eventually affect the equipment in the room. For example, high temperatures, humidity (for example, from water leaks), or lack of airflow can detrimentally affect the equipment. Similarly, alarms, such as smoke and fire alarms, or the status of room openings, are important to determine. While the expense of replacing server room components if they fail is great, currently existing monitoring solutions are not cost effective for smaller-sized companies to implement despite the potential costs of such losses.

**[0011]** Monitoring systems are typically implemented as simple, stand-alone devices with which a user or application may configure and interact. Most appliances allow one or more users or applications to interact with them, but the user or application must typically interact with each appliance separately.

**[0012]** These typical monitoring systems use a centralized application (either an extension to a Network Management System, such as HP OpenView, or a proprietary server or console application). While these mechanisms can be quite effective, they introduce additional costs, through additional software, hardware, configuration, administration, and network bandwidth. Also, the central application/server often introduces a single point of failure into the environment.

**[0013]** Another issue with stand-alone appliances, particularly devices whose primary purpose is to monitor environmental and/or network conditions, is their vulnerability to unreported failure. Specifically, if the monitoring appliance suffers a failure, detection of the

failure typically requires user interaction or polling by an expensive centralized management server. The consequence of non-detection of the failed appliance is an absence in detection of the conditions that the device was responsible for monitoring, coupled with no knowledge of the lapse in coverage.

**[0014]** In the case of an appliance failure, the typical stand-alone appliance lacks any mechanism for the external saving and restoring of data, specifically configuration and historical data. This can add significant overhead and opportunity for errors when a failed device is replaced, as the new device will need to be successfully reconfigured to match the failed device. Mechanisms for saving and restoring configurations for a device on external servers can be implemented, but once again introduces the problem of additional cost and points of failure.

**[0015]** Beyond the application to server rooms and rack mountings of network equipment, various other monitoring systems suffer from the same failures and deficiencies associated with network bandwidth and undetected sensor failure. Further, these monitoring systems may suffer from lost historical data associated with the failure of a sensor.

**[0016]** As such, many typical remote monitoring systems suffer from deficiencies caused by undetected sensor failure and limited communications bandwidth. Many other problems and disadvantages of the prior art will become apparent to one skilled in the art after comparing such prior art with the present invention as described herein.

## SUMMARY OF THE INVENTION:

**[0017]** Aspects of the invention are found in a network-enabled appliance or device. The device may have one or more sensors. These sensors may, for example, measure environmental variables, power-related variables, video or still-images, sounds, or network variables, among others. Further, the network-enabled appliance may send data, alerts, alarms, and/or other notifications associated with the sensors and the measured data.

**[0018]** In addition, the network-enabled appliance may be connected to an interconnected network. Through the interconnected network, the network-enabled appliance may communicate with other network-enabled appliance and/or one or more remote monitoring systems.

**[0019]** The network-enabled appliance may also send data, alarms, and other notifications through various communications means. These means may include telephone networks,

modems, pager networks, other wireless communications means, auditory means, visual means, web-based means, and others.

**[0020]** A further aspect of the invention may be found in a method of communicating between network-enabled appliances. A network-enabled appliance may establish a relationship with a peer network-enabled appliance. The network-enabled appliance may then ping the peer appliance. If the peer appliance does not receive one or more consecutive pings, the peer appliance may determine the state of operability of the network-enabled appliance. In the event of a failure, the peer appliance may send an alert to a remote monitoring facility, a responsible party, or another peer appliance.

**[0021]** The communication may use various protocols including, for example, HTTP, SNMP, TCP/IP, FTP, LDAP, SOAP, UDP, IBM MQSeries messages, and mechanisms including, for example, HTTP POST, CIM events, DMI alerts, database inserts, and log file appends, among others. However, other protocols may be developed or envisaged.

**[0022]** In using a ping method in conjunction with notification when a specified state is measured, the system can monitor a multitude of conditions in a remote location and detect the failure of devices while limiting the bandwidth used for communicating the measurements. As such a remote monitoring system may be established between a cluster of remote network-enabled appliances and facilities at a separate location.

**[0023]** Another aspect of the invention may be found in a cluster of network-enabled appliance. The cluster of network-enabled appliances may establish various peer-to-peer relationships. Further, the cluster of appliance may establish a directory of appliances and their associated capabilities, features, and/or functions. With this directory, the cluster of appliances may share resources. In this manner, the cluster may perform more complex functions. Further, the cluster may perform the function of a failed appliance.

**[0024]** A further aspect of the invention may be found in a remote monitoring system. The remote monitoring system may include one or more network-enabled appliance connected to an interconnected network. Further, a remote system may monitor the one or more network-enabled appliance. Alternately, the remote system may communicate with a single dominant network-enabled appliance. This dominant network-enabled appliance may act as an intermediary between the remote system and other network-enabled appliances within the

cluster. Further, the dominant network-enabled appliance may maintain a directory of the capabilities of the other network-enabled appliances within the cluster.

**[0025]** In addition a backup to the dominant network-enabled appliance may act as a peer observing the dominant network-enabled appliance. In the event that the dominant network-enabled appliance fails, the backup appliance may function as the intermediary and/or maintain the directory.

**[0026]** Another aspects of the invention may be found in a computer or machine-readable medium with an instruction set for performing the method of communication. The medium may take various forms including a CD-ROM, CD-R, CD-RW, DVD, hard drive, floppy disk, removable medium and others.

**[0027]** As such, an apparatus and method for monitoring remote locations are described. Other aspects, advantages and novel features of the present invention will become apparent from the detailed description of the invention when considered in conjunction with the accompanying drawings.

**BRIEF DESCRIPTION OF THE DRAWINGS:**

**[0028]** For a more complete understanding of the present invention and advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings in which like reference numbers indicate like features and wherein:

**[0029]** Fig. 1 is a schematic block diagram of a system for remote monitoring, according to the invention.

**[0030]** Fig. 2 is a schematic block diagram of an exemplary embodiment of a system for remote monitoring according to the system as seen in Fig. 1.

**[0031]** Fig. 3 is a schematic block diagram of an exemplary embodiment of the system as seen in Fig. 1.

**[0032]** Fig. 4 is schematic block diagram of another exemplary embodiment of the system as seen in Fig. 1.

**[0033]** Fig. 5 is a block flow diagram of an exemplary method for use by the system as seen in Fig. 1.

**[0034]** Fig. 6 is a schematic block diagram of another exemplary embodiment of the system as seen in Fig. 1.

**[0035]** Fig. 7 is a schematic block diagram of another exemplary embodiment of the system as seen in Fig. 1.

**[0036]** Fig. 8 is a block diagram of an exemplary embodiment of the network appliance for use in the system as seen in Fig. 1.

**[0037]** Fig. 9 is a diagram depicting an exemplary embodiment of a directory for use in the system as seen in Fig. 1.

**[0038]** Fig. 10A is a schematic block diagram of an exemplary embodiment of the system as seen in Fig. 1.

**[0039]** Fig. 10B is a schematic block diagram of an exemplary embodiment of the system as seen in Fig. 1.

**[0040]** Fig. 11A is a block flow diagram of an exemplary method for use by the system as seen in Fig. 2.

**[0041]** Figure 11B is a block flow diagram of an exemplary method for use by the system as seen in Fig. 2.

**[0042]** Fig. 12 is a schematic block diagram of another exemplary embodiment of the system as seen in Fig. 1.

**[0043]** Fig. 13 is a block flow diagram of an exemplary method for use by the system as seen in Fig. 2.

**[0044]** Fig. 14 is a block flow diagram of an exemplary method for use by the system as seen in Fig. 2.

**[0045]** Fig. 15 is a block flow diagram of an exemplary method for use by the system as seen in Fig. 2.

**[0046]** Corresponding reference numerals indicate corresponding parts throughout the several views of the drawings.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT:

**[0047]** Fig. 1 is a schematic block diagram of the system according to the invention. The system 10 may have a remote monitoring system 12 and a monitoring system 14. Further, the system may have multiple remote monitoring systems 12 connected to one monitoring system 14. Likewise, one remote monitoring system 12 may be connected to a plurality of monitoring systems 14. As such, a remote monitoring system 12 may collect data from multiple monitoring systems 14. Alternately, a monitoring system 14 may send data to a multiplicity of remote monitoring systems 12. Further, a plurality of remote monitoring systems 12 may be connected to a plurality of monitoring systems 14 or in various other combinations.

**[0048]** The remote monitoring system 12 may take various forms. These forms may include a remotely located computer or complex of computers, a phone, a smart phone, an email-enabled phone, a pager, a handheld device, and/or an alarm system, among others. Further, the remote monitoring system 12 may access, monitor, and/or communicate with the monitoring system 14 through various means. These means may include email, web interfaces, pager interfaces, various networking standards, and others.

**[0049]** The monitoring system 14 may take various forms. These forms may include one or more network-enabled devices associated with one or more sensors. Further, the network-enabled devices may be in communication with other network-enabled appliance. The one or more sensors associated with the network-enabled devices may take various forms. These forms may include temperature sensors, pressure sensors, airflow sensors, voltage sensors, current sensors, microphones, cameras, video cameras, network sensors, infrared sensors, motion sensors, and door sensors, among others.

**[0050]** The remote monitoring system 12 and the monitoring system 14 may communicate through various means. These means may include, where appropriate, global networks, wide area networks, local area networks, phone lines, wireless networks, and others. Further, the

remote monitoring system 12 and the monitoring system 14 may communicate using various protocols. These protocols may include TCP/IP, ethernet protocols, SNMP, HTTP, FTP, SOAP, UDP, and IBM MQSeries messages, among others.

**[0051]** The system as seen in Fig. 1 may have various uses. For example, in one exemplary embodiment, the system may be used to monitor a location in which servers and other computers are stored. As such, the user can monitor network assets from remote locations. However, many other embodiments are envisioned. Various other applications may be envisaged. These applications may include military, security, and others.

**[0052]** Fig. 2 is a schematic block diagram of an exemplary embodiment of the system as seen in Fig. 1. The system 30 has various network appliances connected to an interconnected network. This interconnected network may be connected to the remote monitoring system through various means. The network appliances may communicate with peer network appliances through the interconnected network 32. Further, one or more of the network appliances may be in communication with the remote monitoring system 44. This communication may be through the interconnected network 32 or through other means.

**[0053]** The interconnected network 32 may take various forms. These forms may include a global network, wide-area network (WAN), local area network (LAN), and wireless network, among others. Further, various protocols may be used in communicating between appliances. These protocols may include SNMP, HTTP, FTP, TCP/IP, SOAP, UDP, Ethernet protocols, and Bluetooth protocols, among others.

**[0054]** The remote monitoring system 44 may communicate with one or more of the network appliances through the interconnected network or through various other means. These other means may include wireless means and other networking means. For example, these means may include a global network, a dedicated connection, a phone system, a pager system, a modem and a wireless phone system, among others. For example, the network appliances may send data through an interconnected network using an HTTP POST method or an FTP method. Alternately, the network appliances may send a text pager message to a responsible party notifying them of an alarm condition. In another example, the system may make phone calls to responsible parties.

**[0055]** A network appliance may take various forms. In one exemplary embodiment, the network appliance is a device that can perform a well-defined set of functions and which is connected to a network. The device may include software to monitor, configure, control and communicate the results of its functions. Further, the device may be connected to an interconnected network. The device may also be configured, monitored and controlled from a remote location.

**[0056]** A grouping of network appliances may function as a cluster. In this case, a cluster refers to a collection of the interconnected network appliances that may act as a single logical entity. The cluster may be associated in a logical theme or be grouped to facilitate user interaction, among others. This clustering or grouping as a single logical entity may take various forms. These forms may include clustering devices associated with a specific location, a room, a building, a user, a function, a purpose, a network region, a group of users, a responsible party, a remote monitoring location, and/or a servicer, among others.

**[0057]** In one exemplary embodiment, the network appliances may be used to monitor a server room or location. Each network appliance may serve a specific function, monitor a specific variable, or sense an output or environmental state, among others.

**[0058]** For example, one network appliance may be established to monitor environmental conditions such as airflow and temperature. Another network appliance may take the form of a camera. Still further, a network appliance may monitor the state and quality of the network. In a further example, a network appliance may be used to monitor the availability and quality of electrical power. In one embodiment, one or more of these various network appliances may be located throughout a room. For example, several temperature monitors may be placed in various points in a room to acquire data associated with the temperature profile of the room. In another example, several network appliances may be placed in a server rack to monitor airflow, temperature profiles, and electrical quality within and around the rack. In this case, the network appliances may communicate with each other or communicate with a remote monitoring system. In this manner, data associated with the location, may be transferred to the remote monitoring system.

**[0059]** Further, these network appliances may be configured to have alarm settings. The appliance, once an alarm condition is achieved, may send an alert, either to other network

appliances or to the remote monitoring system. In this manner, a complex behavior may be established such that when an alarm condition is achieved by one network appliance, other network appliances send their information to the remote monitoring system or respond accordingly. In one exemplary embodiment, a door sensor network appliance may be used to monitor entry to the server room or entry into the server rack. Once the alarm condition is achieved or once the door is opened, the door sensor network appliance may send a message or an alert to the other network appliances. The other network appliances may respond by sending further information to the remote monitoring system or by performing some other function. For example, once the door sensor network appliance is activated, or an alarm condition is achieved, the door sensor network appliance may send a message to a camera network appliance. The camera network appliance may take a picture of the person entering the door and the network appliance may then send that picture to the remote monitoring system or alternately may send the picture to another network appliance. The other network appliance may function to send the information or alert a user through another system such as a phone system, a pager, or through a modem.

**[0060]** The complex behavior may be achieved through peer-to-peer network appliance communications. Fig. 3 is schematic block diagram depicting an exemplary embodiment of a network appliance communication. According to the invention as seen in Fig. 1. For example, a set of network appliances may be connected to an interconnected network. These appliances may establish communication links between the various network appliances.

**[0061]** In one exemplary embodiment, a network appliance will periodically ping a peer appliance. If the peer appliance does not receive an expected ping, it may establish that the pinging appliance is inoperable. In this manner, failure of an appliance may be quickly detected.

**[0062]** Further, once a failure is detected by the peer appliance, the peer appliance may notify the remote monitoring location or another network appliance of the failure of the first network appliance. With this information, the other network appliances may compensate for the failure, and/or take-on the functionality of the failed device, among others. Similarly, the remote monitoring location and/or a responsible party may respond appropriately.

**[0063]** In one exemplary algorithm, a network appliance may be assigned to monitor several other network appliances. A network appliance may be configured to ping a multiple of other

network appliances and receive pings from another set of network appliances. A network appliance may ping those that are pinging it and others that are not pinging it, or be configured to ping only those that are not pinging it. As such, various algorithms may be established that facilitate peer-to-peer failure detection.

**[0064]** The peer-to-peer communication system may also be used to send alert messages through the network. The review system may also be used to send data, establish various configurations of the system, create complex behaviors and establish a communication with a remote network, among others.

**[0065]** In one exemplary embodiment, a network appliance A may be monitoring a network appliance B, C and D. As such, network appliances B, C and D may ping network appliance A. Alternately, network appliance A may ping network appliances B, C and D.

**[0066]** If network appliance A should fail, be shut down or be removed from the system, devices B, C and D may learn of the device failure or shutdown. For example, if device B were to ping device A and not receive a response, device B may establish that device A is no longer in service. Alternately, if device A were periodically to ping to device C, and the periodic pinging were to cease, device C may establish that device A was no longer in service. In another instance, device A may send a special ping to notify of an impending shutdown event or an expected shutdown event. As such, device B, C, and D may establish that device A is no longer in service. Devices B, C, or D may send notification to the remote monitoring system of the failure or shutdown of device A. In a further example, device B, C, and D may communicate such that only one device sends the failure notice.

**[0067]** Further, device B, C, and D may establish new communication links and a new peer-to-peer review relationship, as seen in Figure 4. For example, appliance B may communicate with appliance C instead of appliance A. Because appliance D no longer requires the resources to monitor appliance A, it may establish a new monitoring of device C. In this manner, the peer-to-peer review may be automatically reconfigured.

**[0068]** In another exemplary embodiment, a new appliance G may be added to the system and/or linked to the network. Device G may establish a peer-to-peer review with appliance B. Further, it may attempt to establish a peer-to-peer review with device D. In one exemplary embodiment, device D may have the option of refusing the peer-to-peer review based on D's

resources, the number of peers that D is already monitoring or being monitored by, and/or other factors. As such, G may then establish a peer-to-peer review relationship with network appliance F. Further, appliances may decide to end the peer-to-peer review. For example, network appliance D may decide to end its review of appliance F. This decision may be based on the appliance's capabilities, the number of other peer-to-peer review relationships, network resources or other factors. Alternately, network appliance F may decide to end its peer-to-peer review relationship with D. This decision may be made for similar reasons.

**[0069]** As such, peer-to-peer relationships may be automatically reconfigured, may be used to monitor the state of various other peer-to-peer appliances, may be used to transfer data between appliances and to establish complex behaviors across appliances, among others.

**[0070]** Peer-to-peer review process may use various protocols to establish communication. These protocols may include FTP, SNMP, HTTP, SOAP, UDP, and TCP/IP, among others.

**[0071]** Fig. 5 is a block flow diagram of an exemplary method for establishing communication for the peer-to-peer review process. The method 50 may be performed by a network appliance. The network appliance may broadcast to find other network appliances on the network as seen in block 52. However, the appliance may employ one or more of a variety of mechanisms to determine the presence of other appliances. For example, the mechanisms may include end-user configuration, multicasting, subnet broadcasting, directory service queries, and subnet address walking, among others.

**[0072]** The network appliance may then ping and/or poll one of the other network appliances found on the network, as seen in the block 54. This ping may take various forms. For example, the ping may use the protocol of an HTTP POST message. The ping may include information such as, for example, the serial number of the requesting appliance, the planned period of time before a next ping, the IP address and hostname of the requesting appliance, and a list of SNMP target addresses for SNMP traps. However, the ping may take various forms including, for example, HTTP, SOAP, SNMP, TCP, UDP, FTP, and IBM MQSeries messages, among others.

**[0073]** The peer device may receive the ping, determine whether it has the resources to establish a peer-to-peer review process and send a response. That response may be received by the network appliance, as seen in a block 56. The response message may include various data. This data may include data similar to the data above and/or may be associated with the

functionality of the location of the device, the address of the device, a desired periodicity of future pings, and acceptance of the relationship, among others. The response may use various protocols including those listed above, among others.

**[0074]** If the peer device accepts the peer-to-peer relationship, the network appliance may wait a given period as established in a communication between the network appliance and its peer, as seen in a block 60. Then, a network appliance may ping the peer again, as seen in a block 54. The peer device may decide whether a message needs to be sent back in response. As such, peer-to-peer review is established.

**[0075]** In one exemplary embodiment, a network-enabled appliance may broadcast across an interconnected network to find address of peer appliances. For example, the network-enabled appliance may send a subnet broadcast. Peer appliances may respond to this broadcast. The network-enabled appliance may then selectively ping one of the responding peer appliances. The network-enabled appliance may for example use an HTTP POST message or an FTP message with information regarding the address of the peer appliance and/or the periodicity of future pings. In addition, the message may contain information about the functionality of the network-enabled appliance, and/or information associated with the algorithms associated with the functionality of the network-enabled appliance. The peer appliance may respond with a message. The message may, for example, use an HTTP Post, FTP, and/or SNMP message, among others. The message may include information associated with acceptance of the peer relationship, the periodicity of future pings, and/or the functionality of the peer device, among others. The network-enabled appliance may then selectively periodically ping the peer appliance.

**[0076]** In one exemplary embodiment, an appliance may, optionally, only "ping" appliances that it is configured to watch and which are not currently "pinging" it. Since a peer appliance is pinging the network appliance periodically, the absence of pings from the appliance can be used to detect its failure. If an appliance is intentionally shutdown, the appliance may issue a special "ping" to each of the devices "pinging" it and/or being "pinged" by it to indicate its plan to shutdown. This may be used to prevent those devices from reporting a planned shutdown or restart as a failure.

**[0077]** In any case, an appliance may be found to have failed if a) a "ping" from the appliance is significantly overdue, or b) one or more attempts to "ping" the appliance fail. When a failure is detected, e-mail addresses or other contact mechanisms supplied by the appliance may be notified. Additionally, SNMP traps (with their agent address set to the IP address of the missing appliance) may be sent to the target SNMP addresses supplied by the appliance. Optionally, the notifications may also be sent to the e-mail and SNMP addresses associated with the failure-detecting appliance (particularly if the failed appliance did not supply this data).

**[0078]** With this algorithm, a network-enabled appliance may establish a peer review relationship with other network-enabled appliance. Further, the network-enabled appliance may selectively establish more than one peer review relationships. In addition, an algorithm may dictate the establishment of a number of peer-to-peer relationships.

**[0079]** In this manner, if a peer device is expecting a periodic ping from a network appliance, it may periodically establish the operational state of the network appliance. If a ping is not received, or a series of pings is not received, the peer device may establish that the network appliance is not operating.

**[0080]** A variation of the peer-to-peer ping may be used for an appliance to home communication. For example, each appliance may be configured to "ping" one or more host web servers. In this case, the appliance does not detect or report outages of the targeted servers, but an application on those servers uses the information reported through the ping to know when to report an appliance outage and to whom to report the outage.

**[0081]** Other embodiments of these mechanisms may use various protocols for "ping" implementation including HTTPS, SOAP, SNMP Traps, proprietary TCP or UDP implementations, and IBM MQSeries messages, among others, as well as other alarm notification mechanisms including HTTP POSTs, CIM Events, DMI Alerts, database INSERTs, and log file append, among others.

**[0082]** The network appliances may communication with the remote monitoring system through various methods. These methods may include a pager network, telephone network, wireless network, global interconnected network, and dedicated line, among others.

**[0083]** In an exemplary embodiment, a periodic message may use an HTTP POST method. Similarly other communications between appliances and between appliances and the remote location may use an HTTP POST method. The method may take a form similar to the following.

POST/ *message_type* HTTP/1.1
Host: *000.000.0.000:00*
User-Agent: *Software/version*
Accept: */*
Accept-Encoding: gzip
Accept-Language: en
VARIABLE1 = 1%VARIABLE2 = 2%VARAIBLE3 = value

**[0084]** The variables may contain information associated with the network appliance type, software version, network ID, hostname, devices, sensors, and other data.

**[0085]** In another exemplary embodiment, messages may be sent using an FTP method. As such, a message may take the form of a text file placed on another appliance or server and appear as:

VARIABLE1 = 1

VARIABLE2 = 2

VARIABLE3 = value

**[0086]** These methods may also be used to transfer image, sound, and other data. In addition, other methods, mechanisms, and protocols may be used to send, transfer, and/or post data.

**[0087]** Fig. 6 is a schematic block diagram of an exemplary embodiment of a system for communicating between the remote monitoring system 72 and network appliances 74, 76, and 78. The system 70 may establish communication between the remote monitoring system 72 and each of the network appliances A, B and C 74 76 78. The remote monitoring system 72 may poll each of the devices. Alternately, each of the devices 74 76 78 may relay information to the remote monitoring system 72.

**[0088]** The communication between the remote monitoring system and the network appliances may take various forms. These forms may include those listed above, among others.

**[0089]** Further, the remote monitoring system 72 and network appliances 74 76 78 may communicate through various protocols. These protocols may include HTTP, FTP, SNMP, SOAP, UDP, TCP/IP, and others.

**[0090]** In an alternate embodiment, remote monitoring system may be configured to communicate with one, two, or less than all of the network appliances. Fig. 7 is schematic block diagram of an exemplary embodiment of a system for communicating between the remote monitoring system 92 and a cluster of network appliances. The system 90 may include a set of network appliances 94 96 100 102 104, connected to an interconnected network 98. The remote monitoring system 92 may be connected to one or more of the network appliances 94 96. However, the remote monitoring system may or may not be connected to the interconnected network 98 connecting each of the appliances 94 96 100 102 104.

**[0091]** Remote monitoring system 92 may communicate with the one or more network appliances 94 96 through various means. These means may include those listed above among others. For example, the remote monitoring system 92 may communicate with network appliance D 94 through a global network, WAN, wireless network, satellite network, dedicated connection and phoneline, among others.

**[0092]** This method of communication between the remote monitoring system 92 and the one or more network appliances 94 96 in conjunction with the peer-to-peer review communications method may permit redundancy in the communications link between the network appliances connected to the interconnected network 98 and the remote monitoring system 92. For example, network appliance D 94, may, through the interconnected network 98 establish a peer-to-peer review communications with network appliance E 96. Further, the network appliances D 94, and network appliance E 96, may have a means of communications with the remote monitoring system 92. If the network appliance D 94 were to fail, the network appliance E 96 may establish communications with the remote monitoring system 92. As such, network appliances A, B and C, through the interconnected network 98, may communicate with a network appliance E 96, which in turn can communicate with the remote monitoring system 92. In this manner, network appliances A, B, and C maintain communications a link with the remote monitoring system 92.

**[0093]** In one exemplary embodiment, a floating IP address may be used. Network appliance D 94 may establish and take ownership of the IP address. If network appliance D 94 were to fail,

network appliance E 96 could take over the IP address and establish itself as the owner. In this manner, the remote monitoring system 92 would maintain communications with the appliances connected to the interconnected network 98 without reconfiguration. In an alternate embodiment, network appliance E 96 may send a message to remote monitoring system 92 indicating the change in the operation status of network appliance D 94. Further, the network appliance E 96 may send a message to remote monitoring system 92 establishing itself as the owner of the communications link to network appliances A, B and C.

**[0094]** In another exemplary embodiment, network appliance D 94 and network appliance E 96 may use differing communication means to reach a remote monitoring system 92. For example, network appliance D 94 may be connected to a global network. In the event of D's failure, network appliance E 96 may have a modem that may call the remote monitoring system 92. Still further, network appliance D 94 and network appliance E 96 may be connected to the remote monitoring system 92 via the same means, but use differing protocols in their communication with remote monitoring system 92. For example, network appliance D 94 may use an HTTP POST protocol to communicate with the remote monitoring system 92 and network appliance E 96 may use an FTP protocol.

**[0095]** Fig. 8 is a block diagram of an exemplary embodiment of a network appliance according to Figs. 1 and 2. A network appliance 110 may have a processor 112, a programmable circuitry 114, a network interface 116, sensors 118, storage 120, clock 134, and a modem 136. However, the network appliance 110 may have all, some or none of these features. Further, the network appliance may use various items in varying combinations to enable varying functionality.

**[0096]** The processor 112 may take various forms. These forms may include microprocessors and other circuitries. The processor 112 may take various operating instructions and/or data and use this information in conjunction with the programmable circuitry 114, the network interface 116, sensors 118, one or more storage mediums 120, a clock 134, a modem 136, and others, to enable the functionality of the network appliance and further establish communications with peer appliances and/or their remote monitoring system. Further, the processor 112 may be functional to operate with a Java-based operating system. In addition, the processor 112, in conjunction with the operating system, may function as a server and/or a web-based server.

**[0097]** The programmable circuitry 114 may take various forms. These forms may accept programming from various means including keyboards, graphic user interface devices, handheld devices, across the network interface and others. In this manner, the functionality of the network appliance may be adapted.

**[0098]** The network interface 116 may take various forms. These forms may include ethernet, wireless ethernet, Token rings, Bluetooth communications means, and modem and phone line, among various other networks and communications interfaces. Furthermore, the network appliance 110 may have more than one network interface connected to similar or differing communications means. For example, one appliance may have a connection to a private ethernet network and an interface connection to a wide area network. Alternately, another appliance may have a network interface connection to a private ethernet network and a wireless ethernet interface. As such, various appliances may have functionality associated with the network interfaces 116. For example, a network appliance with both a private ethernet network interface and a wireless interface may communicate with wireless sensors and communicate the sensor data to other appliances on the private network. In another example, an appliance may have both a private ethernet network interface and a WAN interface. As such, the appliance may function to communicate information from and to appliances on the private network to and form remote locations. However, various combinations and functionalities associated with one or more, similar or varying network interfaces may be envisaged.

**[0099]** Further, the sensors 118 may take various forms. These forms may include temperature sensors, pressure sensors, electric quality sensors, airflow sensors, microphones, cameras, video cameras, infrared cameras, door sensors, motion sensors, and network sensors, among others. One or more sensors 118 may be included in the network appliance. Alternately, the network appliance may not have a sensor 118. In another embodiment, the network appliance may have an audio speaker or visual output. Moreover, the sensor or sensors 118 may or may not be encompassed within the network appliance 110. As such, the sensor or sensors 118 may be integrated in the network appliance 110 or external to the appliance. Further an external sensor may be connected exclusively to the appliance 110, such as, for example, an external temperature sensor, a motion detector, or other sensor connected through a dry-contact cable, among others. Alternately, the sensor or sensors 118 may be external to the appliance 110 but connected to more than one appliance 110, such as, for example, a UPS with multiple dry

contact terminals, among others. Furthermore, the sensor or sensors 118 may be external to the appliance with a wireless connection that may or may not be monitored by one or more appliances in a cluster of appliances, such as, for example, a wireless temperature sensor, a network device monitored through SNMP, and others. Individual sensors that can be monitored by more than one appliance are subject to the load balancing among appliances, dynamic allocation between appliances, and appliance fail-over coverage.

**[00100]** The storage medium 120 may take various forms. These may include RAM, ROM, Flash memory, hard drives, floppy drives, removable drives, DVD, CD, and memory sticks, among others. The storage medium may hold various operational instructions, data and other information. This information may include networking and communications instructions 122, alarm and alert rules 124, peer-to-peer communication instructions 126, appliance to home communication instructions 128, various directories 130, and data 132, among others.

**[00101]** The network and communications instruction 126 may include implementations of various protocols, operating instructions for network interfaces 116 and/or modems 136, and other instructions for communications. Further, the storage medium 120 may hold instruction sets for interpreting messages sent in various protocols. These instruction sets may be written as a CGI, Java servlet, ASP, JSP, or PHP script, among others. Further, these instruction sets may enable the network appliance to function as a wed-based server. For example, the instruction sets may be used to parse HTTP POST messages, receive FTP messages, and/or interpret messages sent using other protocols, methods, and mechanisms.

**[00102]** The storage medium 120 may also have alarm rules 124 and other algorithms, thresholds, and setpoints. These may be used to indicate values of parameters at which notification is desired by a responsible party.

**[00103]** In addition, the storage medium 120 may have peer-to-peer 126 and appliance-to-home 128 communications instructions. These instructions, for example, may direct the communication and communication methods for various purposes with peer appliances and/or remote locations.

**[00104]** Further, directories 130 and other data 132 may be held in the storage medium. The directory 130 may contain information associated with appliances, addresses, hostnames, software, software versions, device types, device data, and others. Further, the directory may be

shared or may be a replica of a shared directory. The data 132 may or may not be communal, shared, and distributed. The data 132 may, for example, be values of sensors, lists such as SNMP trap targets, email notification lists, phone and pager numbers, and others.

**[00105]** In addition, a network appliance may have a clock 134. This clock 134 may take various forms, including analog, digital, and other. The clock 134 may be used in conjunction with the sensors to establish a time at which a measurement is taken.

**[00106]** Further, the network appliance 110 may have a modem 136 or other communication means for connecting across a phone line or other wired or wireless communications means. This may or may not be similar to the network interface 116.

**[00107]** In one exemplary embodiment, the network appliance may function to measure temperature at a point in a server room. The network appliance may, for example, have a processor 112, a programmable circuitry 114, a network interface 116, a temperature sensor 118 and various storage mediums 120. The network appliance may function to take periodic temperature measurements. Further, the network appliance may periodically ping one or more peer appliance to establish a cluster behavior. Further, the network appliance may function to deliver temperature data periodically or on request to either a peer appliance or to the remote monitoring system.

**[00108]** In an alternate embodiment, the network appliance may have a processor 112, a programmable circuitry 114, a network interface 116 and a modem 136. The network appliance may use the networking interface to establish peer-to-peer communications with other appliances on the system. Further, upon alert from another appliance on the system, a network appliance may activate the modem and establish a new communications link with a remote monitoring system. Alternately, the modem may be used to send pages, make phone calls, or perform other communications functionality to alert a responsible party as to the condition of a peer appliance.

**[00109]** One exemplary method of establishing complex interactive behavior between network appliances such as the activation of the modem in response to an alert in a peer appliance is to use a device directory. Fig. 9 is a block diagram of an exemplary embodiment of a device directory. A device directory may hold a device identification, information as to the supported activities of each device associated with the device identification, and various other data associated with the device and/or its functionality.

**[00110]** The device directory may be established through various means. These means may include a broadcasting and/or pinging of other devices found on the interconnected network. Peer devices may communicate with each other information associated with those devices, the supported activities of those devices, and the data associated with the device and supported activity.

**[00111]** These communications and the directory may have various data. These data may include network addresses of appliance, hostname, appliance model, appliance software version, appliance devices and sensors, functionality and/or capabilities of appliances, algorithms, setpoints, tasks, among others. Further the data may include information about the appliance devices and sensors including, for example, local device IDs, device types, device label, device location, and various device-type specific attributes. The network appliance may also be programmed to report its data to directories on other devices upon restart, shutdown, and other events.

**[00112]** Further, network appliances may be programmed to support queries for returning attributes and attributes of supported devices. The network appliances may be programmed to make queries of other appliances. In addition, the appliances may support device and appliance ID validation to allow for the detection of stale references to deleted devices.

**[00113]** The directory structure may enable network appliances to monitor devices and sensors on other network appliances and/or peer appliances. As such, a network appliance may act in response to the value of a variable on another appliance. For example, a camera enabled network appliance may monitor a door sensor on another network appliance. Further, the camera enabled network appliance may send, post, or transfer an image in response to the opening of the door.

**[00114]** Alternately, a network appliance may direct the behavior of another device. For example, using the directory an appliance may determine the address of another appliance with email capabilities and direct the sending of a message through that other appliance.

**[00115]** In another example, a door sensor threshold may be defined on an appliance, and offer the option of a multi-selection list of door sensors on different appliances registered with the directory, as well as a multi-selection list of cameras on various appliances. The resulting threshold would allow for a door-open on any of the door sensors to result in the generation by the appliance of e-mail with pictures captured from one or more different cameras.

**[00116]** In a further example, a panel for configuring email content for sensor alerts could offer an add/remove style pair of list boxes to allow control of the addition of the current values of various sensors from various appliances in the email.

**[00117]** In another example, a temperature sensor threshold may be defined on an appliance, and offer the option of a multi-selection list of temperature sensors on various appliances. As a result, a single threshold definition would be applied to these multiple sensors, and only a single stream of SNMP alerts and/or emails would be generated, in contrast with many messages from the appliances with the temperature sensors. Notification emails may include the current values of all the selected sensors, as well as an indication as to whether a given sensor was in error or not.

**[00118]** To support these activities, each appliance may support a HTTP POST based interface for querying the current values of multiple attributes. The interface may query by device unique ID. For cameras and other special sensors, a HTTP POST based interface may be used to return images, streaming data, sound streams, or other data types.

**[00119]** Further, an HTTP POST based configuration interface may allow for the definition of thresholds on the appliance that would notify the configuring appliance when a violation occurred. Appliances may support multiple instances of these thresholds per attribute. In addition, an HTTP POST based threshold violation notification mechanism may be used to notify the threshold's remote owner of the violation.

**[00120]** Also, an HTTP POST based interface may allow appliances to validate the thresholds remotely configured on the appliance. This may be accomplished by querying the appliance which set the threshold if the threshold is still valid. Appliances may use this interface whenever there was a lapse in availability, such as a network outage or a reset of the appliance.

**[00121]** Further, an HTTP POST based interface may allow querying of the status of thresholds remotely configured on the appliance, to allow synchronization between the appliance that configured the thresholds and the appliance which implements them. The querying may be used, for example, following a restart or a network outage.

**[00122]** In addition, an HTTP POST based interface may be used for setting the output values for output devices. These devices may also support a current value query interface.

**[00123]** While the HTTP POST based interface has been used for exemplary purposes, various other interfaces can be envisaged that perform various functionalities. These interfaces may use other protocols including FTP, SNMP, CIM, SOAP, proprietary UDP or TCP, or LDAP, among others.

**[00124]** By allowing the specification of more than one directory appliance/service, a measure of fault tolerance is achieved. To help with fault recovery, directory appliances may be common to all members of a set of appliances, and may be configured to know of each other. When a directory service appliance is activated, it may attempt to contact one of its peers, and request a list of all appliances known by the peers. This list may be used to update the list of appliances known by the directory appliance and, in turn, used to request each of those appliances to re-publish their data to the appliance. Appliances which are successfully contacted but refuse to republish may be discarded.

**[00125]** In order to support security, each directory appliance may support the option of configuring an access user-ID and password, which may be configured on each appliance that attempts to join and use the directory. For added security, passwords unique to each appliance that attempts to use the directory may be required. Other embodiments may support any of a variety of security servers (LDAP, Kerberos, DCE, NIS) or mechanisms (digital signatures, public-private key encryption).

**[00126]** In an alternate embodiment, a single network appliance may establish a master directory. The master directory network appliance may poll other appliances found on the network and receive information which may be stored in the directory.

**[00127]** Another means of fault tolerance with the directory appliances may be to implement an IP address based fail-over between the primary and secondary directory appliances. In this way, all appliances would only refer to and interact with a single directory appliance. The implementation of this may involve each of the directory appliances having a distinct IP address, with one of them (at a given moment) also having the IP address assigned to the directory appliance. The primary directory appliance may, by default, have the IP address of the directory appliance and its own distinct IP address. The secondary appliance may possess a distinct IP address. Any updates to the primary appliance may be communicated immediately to the secondary appliance, to maintain synchronization. Meanwhile, the secondary appliance may

regularly poll the primary in order to watch for a failure. If a failure occurred, the secondary appliance may, for example, activate the directory service IP address on itself, send gratuitous ARP resolves to the network to force any ARP caches on the network to recognize the new location of the IP address, and assume the roll of primary directory appliance. When replaced or serviced, the former primary directory appliance may contact the new primary, synchronize directory data, and assume the roll of secondary directory appliance.

**[00128]** Fig. 10A shows a network appliance A with a directory. Network appliances B, C, D and E communicate with network appliance A to establish the directory. These appliances may communicate with the network appliance A through the interconnected network.

**[00129]** Still further, network appliance may poll the network appliance with the master directory to locate resources owned by other network appliances. In this manner, a network appliance may enhance its own functionality by using features and functionality of other network appliances. For example, network appliance B may sense an environmental variable. However, B may not have the capability of sending email through a global network. Network appliance C may not sense environmental variables. However, it may have a connection to a global network. As such, network appliance B can query the directory of network appliance A to learn of the global connection of network appliance C. Network appliance B may then communicate with network appliance C to establish an external link.

**[00130]** In an even more complex exemplary embodiment, network appliance B may sense an environmental variable. Network appliance B may not have image functionality or connection to an external network. As such, network appliance B, upon establishing alarm condition or other condition, for example, may query network appliance A and the directory on network appliance A. Network appliance B may then learn of the resources of network appliance E, D and C. As such, network appliance B may, for example, communicate with a camera based network appliance E . Network appliance E may then send an image through network appliance C through the external network. In this manner, increasingly complex behaviors may be established using the cluster while maintaining the autonomy of the various network appliances. Even further, the directory may be stored on various network appliances.

**[00131]** As seen in Fig. 10B, the directory may reside in network appliance E . For example, E may have established a peer communications with network appliance A. Upon failure or

shutdown of network appliance A, E may have established the need for a new directory. As such, E may have acquired the directory from A, or E may repoll and rebroadcast to discover the device's supported activities and various data associated with those devices and supported activities from the other network appliances connected to the interconnected network. Another method for facilitating the transfer of the directory and any other data required by the cluster as a whole or by various devices within the cluster, may need to establish a master list and a slave list.

**[00132]** Figure 11A is block flow diagram of an exemplary method for building a directory. In the method 140, a network appliance may determine the location of a directory, as seen in a block 142. The directory may be stored on another network appliance. Alternately, the directory may be stored on a server.

**[00133]** In a next block 144, the network appliance may notify the directory device and direct the storage of information associated with the network appliance. This information may include address, resources, sensors, responsibilities, unique identifiers, data, peer relationship data, and responsible parties, among others. Further, the information may include configuration parameters.

**[00134]** In an alternate method, the directory device may initiate contact with the network appliance and request information for storage in a database. Fig. 11B is a block flow diagram of an exemplary method for building a directory. The directory device may locate the network appliance, as seen in a block 146. The directory device may use various means such as address walking, an SNMP trap, querying appliances at known address, acquire peer addresses from known appliances, and others.

**[00135]** As seen in a next block 147, the directory device may request data from the network appliance. The data may include address, resources, sensors, responsibilities, unique identifiers, data, peer relationship data, and responsible parties, among others. Further, the information may include configuration parameters. Then, the directory device may adjust the directory accordingly, as seen in a block 148.

**[00136]** The directory device may take the form of a network appliance. Alternately, the directory device may take the form of a server. Furthermore, the directory device may take the

form of a network appliance with access to a database residing on a server. As such, the directory may be stored on the network appliance, on a server, or network drive, among others.

**[00137]** In a general exemplary embodiment, as seen in Fig. 12, a network appliance A may have a master data A. Network appliance B may be in peer-to-peer communication with network appliance A and may establish a slave data set associated with the master dataset A. This may, for example, be a master and slave directory, or it may take the form of other data mutually useful by A or B or by other appliances on the network. In addition, B may hold the master list (master data B) storing various other information. Further, network appliance C may store slave data for B and, in further redundancy, may store slave data for A. However, the network appliance need not store any slave data nor a master list as seen by network appliance D.

**[00138]** Furthermore, one or more servers may or may not be connected to the network. Data may be stored on these servers. The data may take the form of a directory, a master data, or a slave data, among others. As such, the server and data may take various forms. These forms may include, for example, files on a files server, a database on a database server, and an LDAP server, among others. One or more of the network appliances attached to the interconnected network may be clients of the one or more servers.

**[00139]** In this manner, complex behavior may further take advantage of communal data. For example, a responsible party may desire an email upon a given temperature condition. If one or more temperature sensors exist in the room, an alert rule and the associated pager number or email address or other data may be stored in a community accessible master data list. The information may further be stored by each of the temperature sensor devices as a slave-data set. As such, when the temperature condition is met, the notification may be sent to the responsible party . The temperature sensing device at which the condition is met may chose to poll the master data list to determine how, where or what to do with the information. Alternately, the network appliance may use the slave data list or data set to determine its behavior.

**[00140]** In this manner, redundancy of community accessible information has enabled. Further a user may change the desired information in one location and have that information become universal.

**[00141]** Further a remote monitoring fail-over and load balancing may be implemented. A number of the features implemented by monitoring appliances may be based on the observation

through the network of other device, especially through protocols such as SNMP, CIM, and HTTP. In the presence of multiple appliances, the choice of which appliances monitor which network devices may be associated with the capabilities and capacities of the individual appliances. This fact can be used as the basis for both dynamic allocation of device monitoring tasks and a mechanism for fail-over of monitoring responsibilities if an appliance fails. In addition load balancing, fail-over monitoring, and dynamic allocation may be applied to the monitoring of shared sensors.

**[00142]** In an exemplary method 150 as seen in Fig. 13, responsibilities and/or resources may be reallocated. For example, in the event that a peer device fails, as seen in a block 152, a network appliance may access the directory to determine what resources, responsibilities, and contacts are assigned to the failed device.

**[00143]** The resources may for example be data management, capabilities, functions, and sensors, among others. The failure of a device may diminish the capabilities of a cluster. Alternately, devices relying on the capabilities and functionality of the failed appliance may be informed of the failure. In this manner, appliances relying on the failed appliance may determine, through accessing the directory or other means, whether and how to access an alternate device, notify a responsible party of the loss of capability, and/or establish peer relationships, among other. For example, a device with a modem, may act as a means of paging responsible parties. If this device were to fail, the cluster may loose paging capabilities. Further, peer devices would loose a peer relationship. As such, the cluster would need to find an alternate device with paging capability or an alternate means of communicating, for example, alarms. Furthermore, new peer relationships may be established. However, various examples of resources may be envisaged.

**[00144]** The responsibilities may include monitoring of shared sensors, directory or back-up directory service, data storage service, peer relationships, and alarm monitoring, among others. The network appliance monitoring the failed appliance may reassign the responsibilities. For example, the appliance may poll other appliances to request acceptance of the responsibility. The other appliances may, for example, be found in the directory. For example, the appliance may access the directory to determine which other appliances are capable of communicating with a shared wireless sensor. The appliance may then assign or request acceptance of the responsibility from the other appliance, as seen in a block 156.

**[00145]** Further, the appliance may notify responsible parties of the peer's failure, as seen in a block 158. The appliance may access, for example, the directory to determine who the responsible parties are and how to contact them.

**[00146]** Moreover, the network appliance may adjust the directory, as seen in a block 160. The adjustment may reflect the failure of the appliance, deletion of the appliance, reassignment of responsibilities, and actions taken in response to the failure, among others.

**[00147]** These steps may be performed in various combinations or not at all. Furthermore, various other methods may be envisaged for reallocation of resources, dynamic allocation of responsibilities, and notification of responsible parties. In addition, the method 150 may be performed by a device prior to a planned shutdown or deactivation.

**[00148]** In one example, each appliance in a set of appliances registered with a given set of directory appliances (an "appliance domain") may publish a set of records in the directory describing its capabilities for remote monitoring. Specifically, a record may be defined for each type of remote monitoring containing the quantity of devices that can be supported, the number of devices currently being monitored, the version of implementation of the remote monitoring, and other monitoring-type-specific attributes. Each record may be keyed, for example, by the combination of the appliance's serial number and the type of remote monitoring.

**[00149]** The contents of this capability directory will be used by both configuration tools (to determine what remote monitoring capability is available and if any additional capacity is available) and for responding to failures (since the directory will aid in determining what other devices are capable of being assigned work from failed appliances.)

**[00150]** Appliances registered in a given appliance domain may define the configuration for any remote monitoring as a set of directory records. Each such record may include the type of remote monitoring, the address and identity of the device to be monitored, the appliance serial number of the appliance currently monitoring the device, and any monitoring-type-specific settings.

**[00151]** In one example, when a new device is configured for monitoring, a new record may be added to the configuration directory with no initial appliance assigned. The configuration tool may then query the capability directory for any appliances with the required monitoring

capability and the capacity to monitor additional devices. The resulting list of appliances may then be sorted, based on such priorities as subnet locality to the device, available capacity, and monitoring function level. The configuration tool may then traverse the sorted list, sending requests to each appliance to accept ownership of the monitoring responsibility for the device until an appliance accepts ownership. The accepting appliance may set itself as the monitoring appliance for the device.

**[00152]** When an appliance fails, the peer appliance detecting the outage may query the configuration directory for any records owned by the failed device. If any are found, it may request that the record be set to un-owned (serial number = 0) and may repeat the same allocation algorithm used for initial configuration until a new owner is found. If an appliance is being shutdown or is being removed from the appliance domain, it may repeat this same procedure on its own behalf, assigning its responsibilities to other devices. Furthermore, these methods of reallocation may be applied to monitoring responsibility for shared sensors.

**[00153]** A number of other configuration elements may provide significant benefit if defined in a shared fashion in the directory of the appliance domain. Specifically, shared objects for such things as user accounts and privileges, e-mail notification templates, action response profiles, e-mail notification lists, and SNMP trap target lists would provide benefit.

**[00154]** To provide an efficient mechanism for these objects, the directory client and server implementation may be enhanced to provide and support a configuration subscription mechanism with local, persistent caching of directory records. Specifically, each appliance that has an interest in a given shared object may subscribe to that object on the directory server. This may result in the appliance receiving an initial copy of the record, as well as automatically receiving updates to that record when the "master" is updated. By doing so, the appliance may then be able to use the data without repeatedly requesting the information from the directory server, as well as being able to operate with the cached copy of the data if a network outage or directory server outage occurs. The subscriber list for each directory record may be stored persistently with the record on the directory server, so that an appliance that has been offline can be automatically brought up-to-date when contact is made with the directory server.

**[00155]** Shared configuration objects may be published as named records to the directory server, and may consist of a domain-unique ID, label, type, and list of object-type-specific attribute/value pairs.

**[00156]** Shared objects may include user accounts, email notification lists, SNMP trap notification lists, email notification templates, and action response profiles, among others. User Accounts may simplify the management of access control for a group of appliances, by allowing single user-id/password for all appliances and a way to apply access control to new appliances added to the group. Accounts may support access control lists for accessing specific appliances, devices attached to those appliances, and other shared objects.

**[00157]** E-mail notification lists may allow administration of shared notification lists, so that the various notification actions configured on different appliances can be tailored without the need to interact with each appliance directly. Configuration attributes which refer to e-mail addresses may support both explicit e-mail addresses and symbolic references to shared e-mail notification lists.

**[00158]** SNMP trap notification lists, as with e-mail, where SNMP trap targets are specified may support explicit target lists and symbolic references to shared SNMP notification lists.

**[00159]** E-mail notification templates may be user-definable "form letters" for e-mail alarm notifications, allowing the user to indicate what text to send and supporting macros for embedding various attributes of the appliance and its devices and sensors. Allowing multiple appliances to share these definitions may provide simple and consistent tailoring of these notifications across many appliances.

**[00160]** Action response profiles may define a set of responses, including repeated actions and escalation, to alert conditions detected through thresholds or other means. Many customers with multiple appliances may allow these responses to be consistent and easily updated across their appliances.

**[00161]** The shared objects and directory resources, among others, may be used to enable bulk configuration of devices. In a method 170 as seen in Fig. 14, a user may define a configuration that is to be applied to multiple devices, as seen in a block 172. The configuration may include

action response profiles, email notification templates, SNMP trap notification lists, email notification lists, and shared configuration objects, among others.

**[00162]** The user may then access the directory or other storage device and store the configuration, as seen in a block 174. For example the user may access the directory device, proxy device, or primary appliance, among others.

**[00163]** Next, the configuration may be distributed as seen in a block 176. The distribution may be accomplished by polling appliances to which the configuration is assigned, transferring the data to the appliance upon request from the appliance, and other methods.

**[00164]** Furthermore, the shared objects and directory resources, among others, may be used to build complex appliance behavior. For example, as seen in Fig. 15, a method may be established for using shared resources. As seen in method 190, an appliance may enter an alarm state, as seen in a block 192. However, this step may or may not be included in the method 190.

**[00165]** The appliance may evaluate an established procedure, as seen in a block 194. The established procedure may be instructions to notify a responsible party, direct the behavior of another device, or notify another appliance, among others. However, this step may or may not be included in the method 190.

**[00166]** The appliance may access the directory as seen in a block 196. A such, the appliance may determine the address of other appliances with desired resources. For example, a door alarm appliance may access the directory to determine the address of a camera appliance. Alternately, a temperature sensor appliance may access the directory to determine the address of a paging enabled appliance. Furthermore, the appliance may access the directory for notification lists, methods, and other shared objects.

**[00167]** The appliance may access resources on other appliances as seen in a block 198. For example, the door alarm appliance may access images on the camera appliance. Alternately, the door alarm appliance may direct the camera appliance to send an image to a responsible party. In another example, a temperature sensor appliance may direct a pager-enabled appliance to send a page to a responsible part. However, various examples of complex behavior may be envisaged.

**[00168]** Further, to support a single, fault-tolerant interface for configuration and application GUIs to interact with the appliance domain as a single unit, support for one or more "floating" IP addresses (similar to the fail-over mechanism described for the directory server) may be implemented. This may allow one of the appliances in the appliance domain to possess a given additional IP address intended for access by external parties (i.e. web browsers, Java applications, etc). As with the directory server, one or more backup appliances on the same subnet may be configured, so that a failure in the primary appliance may result in one of the backup appliances "claiming" the public IP address, allowing uninterrupted service.

**[00169]** Besides supporting public IP address fail-over, the appliances may support proxy of requests to other appliances in the domain. For example, requests to access configuration data or sensor data on a given appliance could either be done by directly interacting with the appliance, or issuing a request through the appliance owning the public IP address. Proxy access may be by appliance serial number, so that DHCP or other unannounced IP address reassignment can be supported. Allowing proxy access may also allow better support for accessing through firewalls (since only the public IP address would need to be "opened"). Support of proxy requests may, in general, use shared user accounts, since the security context of the requesting application would need to be equally meaningful to all appliances in the domain.

**[00170]** As such, a monitoring system is described. In view of the above detailed description of the present invention and associated drawings, other modifications and variations will now become apparent to those skilled in the art. It should also be apparent that such other modifications and variations may be effected without departing from the spirit and scope of the present invention as set forth in the claims which follow.